

# SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN



Homeland  
Security



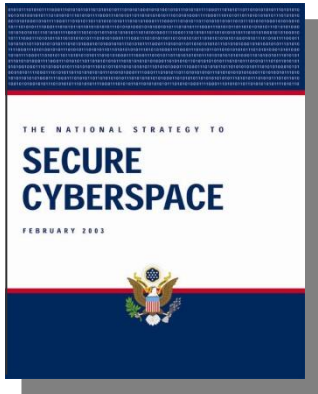
Commerc  
e



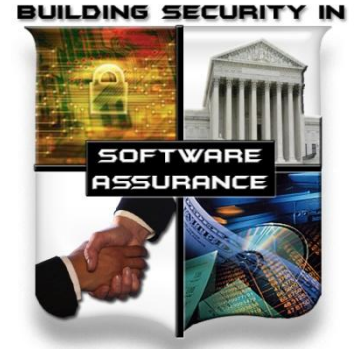
National  
Defense



Next SwA Forum 27 Sep – 1 Oct 2010 at NIST, Gaithersburg, MD



# Software Assurance



## Public/Private Collaboration Efforts in Software Security to Mitigate Software Supply Chain Risks and Improve Incident Management

Aug 17, 2010



Homeland  
Security

Joe Jarzombek, PMP, CSSLP  
Director for Software Assurance  
National Cyber Security Division  
Office of the Assistant Secretary for  
Cybersecurity and Communications

# Software Assurance Panel

- ▶ Joe Jarzombek, Director for Software Assurance, DHS NCSD
- ▶ Bob Martin, MITRE
- ▶ Sean Barnum, MITRE
- ▶ Tom Millar, Deputy Director, US-CERT, DHS NCSD

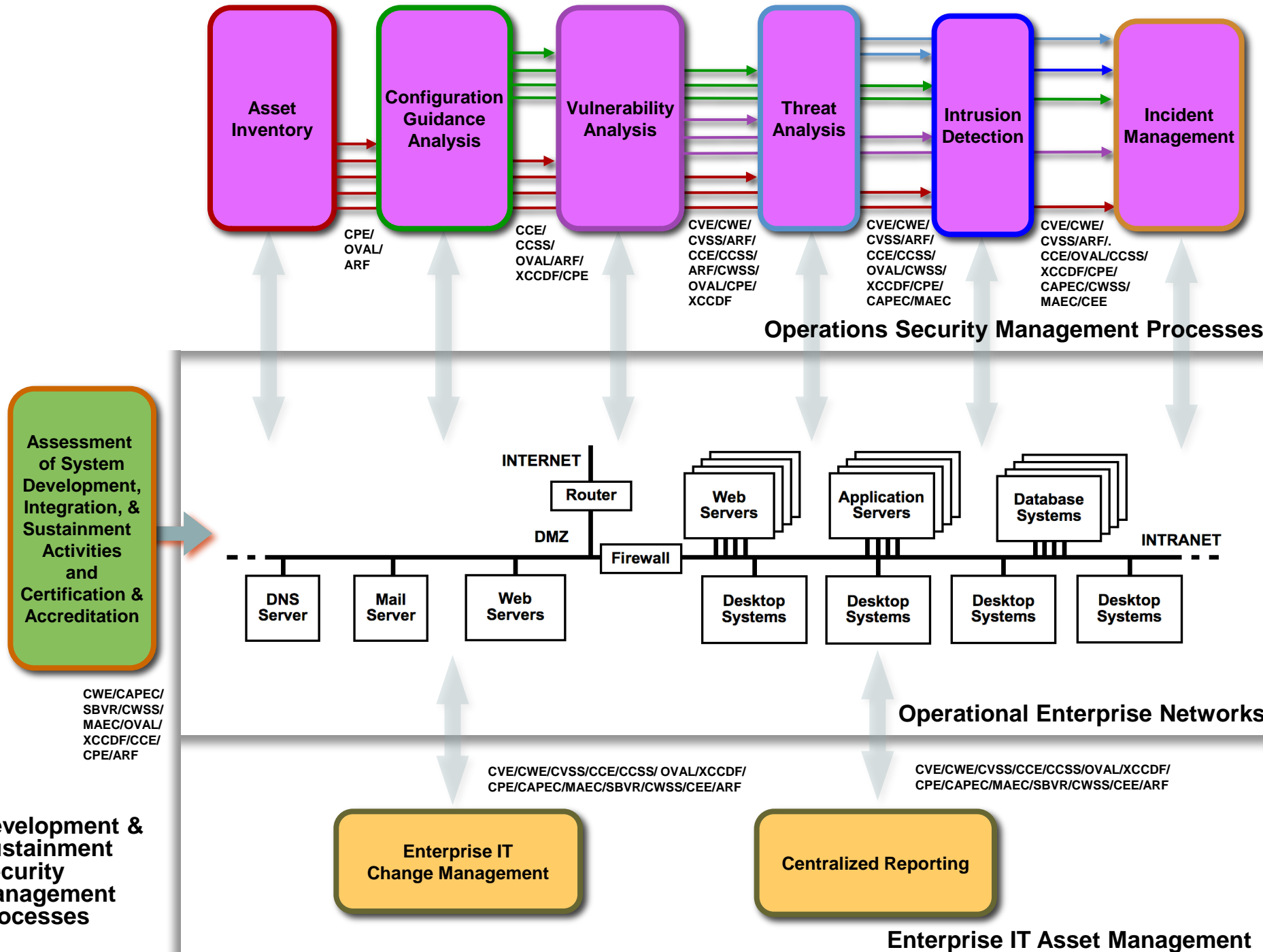
# DHS NCSD Software Assurance (SwA) Program

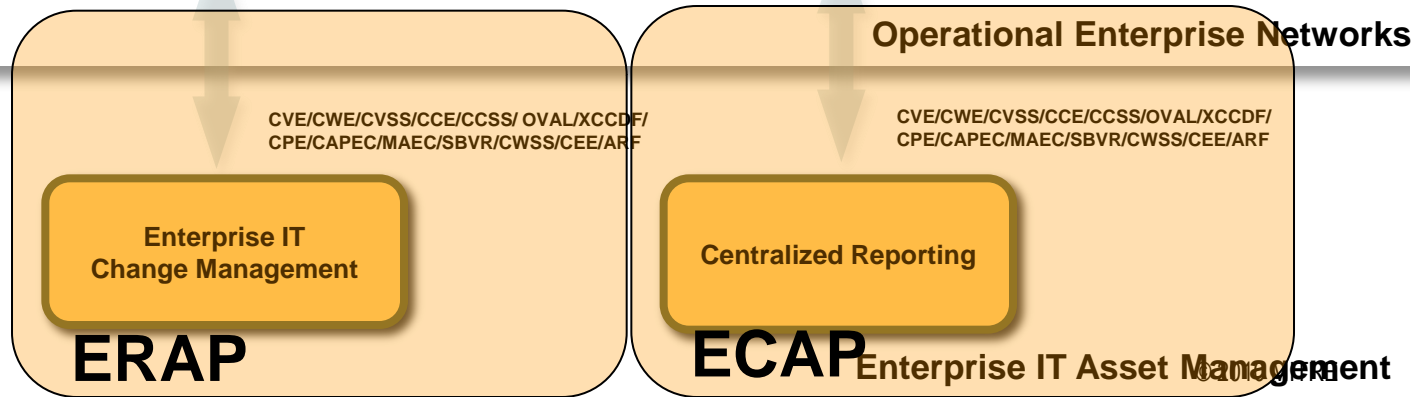
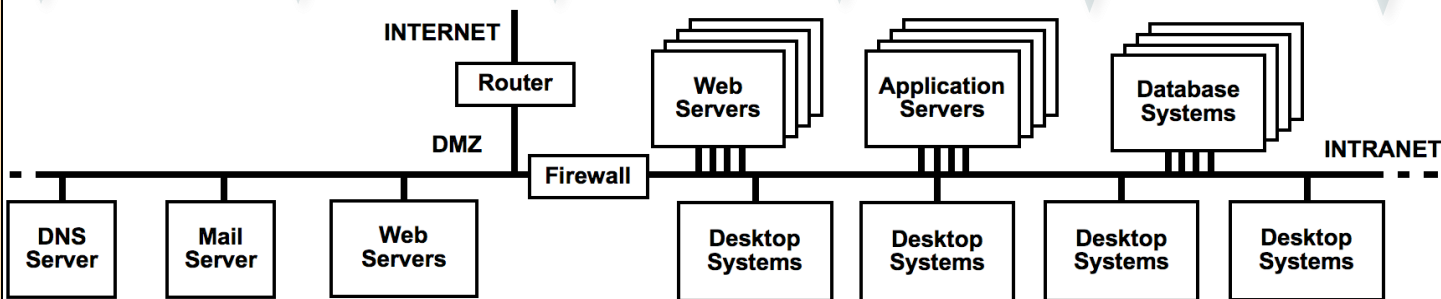
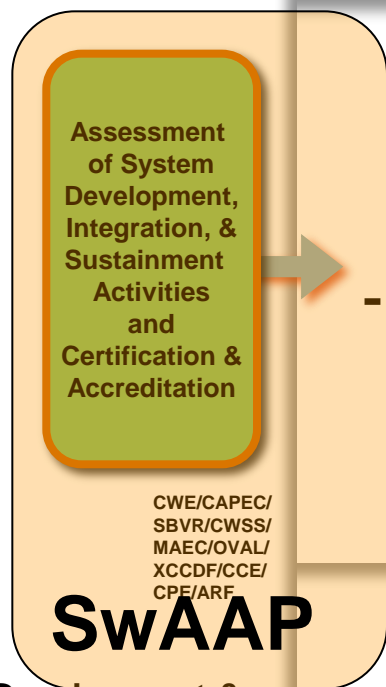
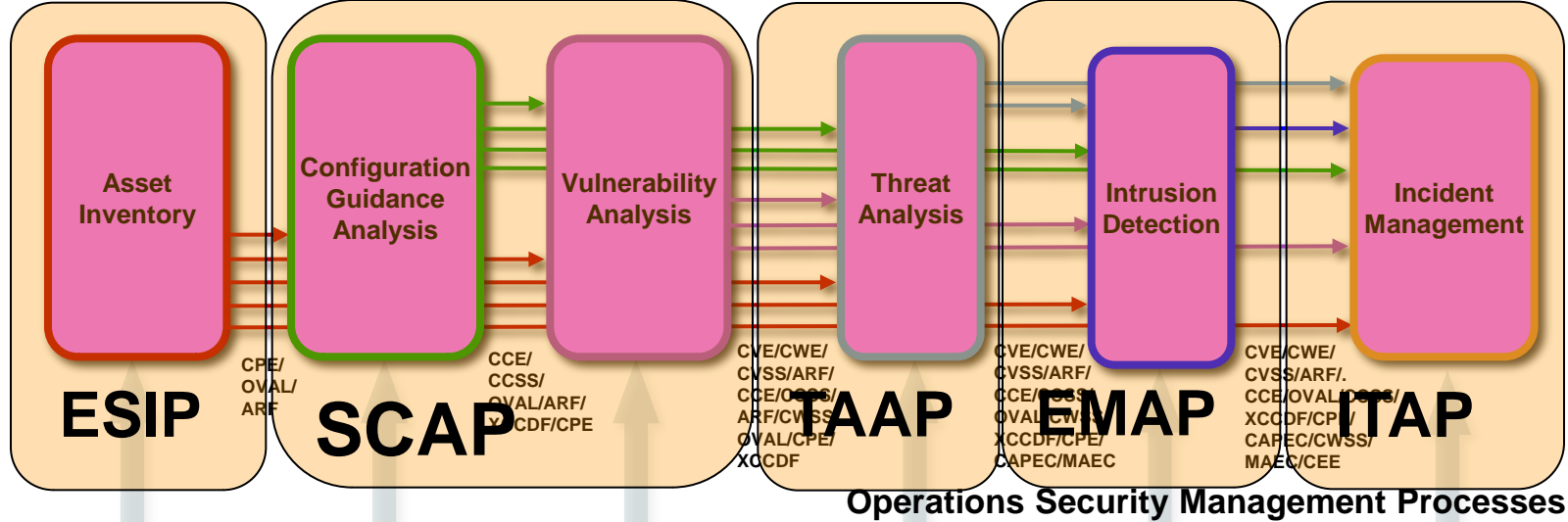
*Through public-private collaboration promotes security and resilience of software throughout the lifecycle; focused on reducing exploitable software weaknesses and addressing means to improve capabilities that routinely develop, acquire, and deploy resilient software products. Collaboratively advancing software-relevant rating schemes*

- **Serves as a focal point for interagency public-private collaboration to enhance development and acquisition processes and capability benchmarking to address software security needs.**
  - Hosts interagency Software Assurance Forums, Working Groups and training to provide public-private collaboration in advancing software security and providing publicly available resources.
  - Provides collaboratively developed, peer-reviewed information resources on Software Assurance, via journals, guides & on-line resources suitable for use in education, training, and process improvement.
  - Provides input and criteria for leveraging international standards and maturity models used for process improvement and capability benchmarking of software suppliers and acquisition organizations.
- **Enables software security automation and measurement capabilities through use of common indexing and reporting capabilities for malware, exploitable software weaknesses, and common attacks which target software.**
  - Collaborates with the National Institute of Standards and Technology, international standards organizations, and tool vendors to create standards, metrics and certification mechanisms from which tools can be qualified for software security verification.
  - Manages programs to facilitate the adoption of Malware Attribute Enumeration Classification (MAEC), Common Weakness Enumeration (CWE), and Common Attack Pattern Enumeration and Classification (CAPEC).

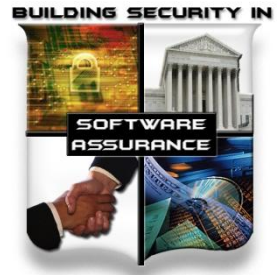








**Development & Sustainment Security Management Processes**



# SOFTWARE ASSURANCE FORUM

“Building Security In”

<https://buildsecurityin.us-cert.gov/swa>



**Homeland  
Security**

Joe Jarzombek, PMP, CSSLP  
Director for Software Assurance  
National Cyber Security Division  
Department of Homeland Security  
Joe.Jarzombek@dhs.gov  
(703) 235-5126  
LinkedIn SwA Mega-Community

# SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN



Homeland  
Security



Commere



National  
Defense



Next SwA Forum 27 Sep – 1 Oct 2010 at NIST, Gaithersburg, MD